Math 522 Exam 6 Solutions

1. Find a reduced residue system modulo 15 consisting entirely of primes.

   The 'standard' reduced residue system is $\{1, 2, 4, 7, 8, 11, 13, 14\}$. *Many of these are primes already, but we need to replace 1,4,8,14, by finding primes congruent to them modulo 15.* $1 + 15 = 16$, *but* $1 + 30 = 31$. $4 + 15 = 19, 8 + 15 = 23, 14 + 15 = 29$. *Hence* $\{31, 2, 19, 7, 23, 11, 13, 29\}$ *is a solution.*

   BONUS: $1 \equiv 1 \cdot 1 \equiv 2 \cdot 8 \equiv 4 \cdot 4 \equiv 7 \cdot 13 \equiv 11 \cdot 11 \equiv 14 \cdot 14$.
   So $31^{-1} = 31, 2^{-1} = 23, 19^{-1} = 19, 7^{-1} = 13, 23^{-1} = 2, 11^{-1} = 11, 13^{-1} = 7, 29^{-1} = 29$.

   An important theorem of Dirichlet's on primes in arithmetic progressions states that you may replace any element from the reduced residue system with INFINITELY many different primes.

2. Fix $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$. Suppose that $R = \{r_i : 1 \le i \le m\}$ is a complete residue system modulo m, and that $S = \{s_j : 1 \le j \le n\}$ is a complete residue system modulo n. Prove that $T = nR + mS = \{nr_i + ms_j : 1 \le i \le m, 1 \le j \le n\}$ is a complete residue system modulo mn.

   The strategy will be to use the main theorem proved in class for this section. To prove that T is a complete residue system, we need to show that any two different elements of T are incongruent, and we need to show that $|T| = mn$.

   Suppose two elements of T were congruent; then $nr_i + ms_j \equiv nr_i' + ms_j' \pmod{mn}$. *Because* $\gcd(m, n) = 1$, *this is logically equivalent (by an earlier theorem) to* $nr_i + ms_j \equiv nr_i' + ms_j' \pmod{m}$ *AND* $nr_i + ms_j \equiv nr_i' + ms_j' \pmod{n}$.

   From the first equivalence, we may conclude that $nr_i \equiv nr_i' \pmod{m}$. *But, since* $\gcd(n, m) = 1$, *we may divide by n to get* $r_i \equiv r_i' \pmod{m}$. *Since r_i, r_i' are in R, they must in fact be the same element of R.*

   From the second equivalence, we proceed similarly. We conclude that $ms_j \equiv ms_j' \pmod{n}$. *But, since* $\gcd(n, m) = 1$, *we may divide by m to get* $s_j \equiv s_j' \pmod{n}$. *Since s_j, s_j' are in S, they must in fact be the same element of S.*

   But then $nr_i + ms_j$ and $nr_i' + ms_j'$ are in fact the same element of T. Hence, any two different elements of T are incongruent.

   We now show that $|T| = mn$. If $nr_i + ms_j = nr_i' + ms_j'$, then in particular $nr_i + ms_j \equiv nr_i' + ms_j' \pmod{mn}$. *But we've already shown this to be impossible in the first part of the problem, hence the elements of T are unequal (i.e. all different). Note: This proof is nontrivial; if* $\gcd(m, n) \ne 1$, *then $|T|$ might not be mn; for example if* $R = \{0, 1\}, S = \{0, 1\}, m = n = 2$, *we have* $T = \{0, 2, 4\}$.

3. Exam grades: 95, 95, 94, 92, 91, 88, 83, 82, 80, 78, 76, 66, 64, 57